UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/601,374	06/23/2003	David John Craft	AUS920030401US1	7981

45327 7590 11/29/2006

IBM CORPORATION (CS)
C/O CARR LLP
670 FOUNDERS SQUARE
900 JACKSON STREET
DALLAS, TX 75202

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 11/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/601,374	CRAFT ET AL.	
	Examiner	Art Unit	
	Carlton Johnson	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 June 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 June 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application papers filed **6-23-2003**.

2. Claims **1 - 21** are pending. Claims **1, 6, 12, 20, 21** are independent.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims **1 - 4, 6 - 8, 10 - 21** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Ellison et al.** (US PGPUB No. **7,082,615**) in view of **Worley, JR et al.** (US PGPUB No. **20020194389**).

Regarding Claim 1, Ellison discloses a method for loading and executing applications securely, comprising:

a) transitioning an attached processor complex (APC) to an isolated state; (see Ellison col. 3, lines 32-35; col. 3, lines 43-45: initiate an isolated state)

b) loading a load image into the isolated APC; (see Ellison col. 3, lines 21-25; col. 3, lines 45-47: load image into isolated region)

e) clearing the load image; (see Ellison col. 3 lines 43-45: initialize (i.e. clear) isolated region) and

f) returning a processor of the APC to a cleared non-isolated state upon completion of the execution of the load image. (see Ellison col. 5, lines 57-59: initialize to isolated and non-isolated state, control and configuration of memory (i.e. non-isolated region))

Ellison discloses the capability to verify a software module (i.e. load image) (see Ellison col. 3, lines 45-47: verifies (i.e. authenticate) load image; col. 5, lines 5-10: execute loaded image), and executing the load module. (see Ellison col. 5, lines 5-10; col. 6, lines 13-18: restricted execution in isolated region) Ellison does not specifically disclose wherein authenticating the load image in the isolated APC. However, Worley discloses:

c) authenticating the load image in the isolated APC; (see Worley paragraph [0049], lines 1-7; paragraph [0129], lines 9-15; paragraph [0139], lines 27-33: authenticating image)

d) if the load image successfully authenticates; (see Worley paragraph [0049], lines 1-7; paragraph [0129], lines 9-15; paragraph [0139], lines 27-33: authentication determination, status successful or unsuccessful)

It would have been obvious to one of ordinary skill in the art to modify Ellison as taught by Worley to enable the capability to authenticate a load image, and determine if load image successfully authenticates. One of ordinary skill in the art would have been motivated to employ the teachings of Worley in order to enable operational control of secure resources without exposing privilege instructions and

registers. (see Worley paragraph [0020], lines 16-21: " ... provide a set of secure-platform management services for operational control of hardware resources that neither expose privileged instructions and privileged registers of the hardware nor simulate privileged instructions and privileged registers. ... ")

Regarding Claim 2, Ellison discloses the method of claim 1, further comprising decrypting at least a section of the loaded image. (see Ellison col. 10, lines 6-8; col. 9, lines 64-65; col. 10, lines 16-19: decryption, subset (i.e. software, loaded image))

Regarding Claim 3, Ellison discloses the method of claim 1, wherein stopping a processor of the APC in an isolated state. (see Ellison col. 3, lines 4-8; col. 4, lines 16-22: isolated and non-isolated, execution and memory; col. 9, lines 52-58: stop processor, fault condition encountered) Ellison does not specifically disclose if authentication of the load image fails, and signaling authentication failure to the MPU. However, Worley discloses wherein if authentication of the load image fails, and signaling authentication failure to the MPU. (see Worley paragraph [0049], lines 1-7; paragraph [0129], lines 9-15; paragraph [0139], lines 27-33: authentication image check and failure status indication)

It would have been obvious to one of ordinary skill in the art to modify Ellison as taught by Worley to enable the capability to determine that authentication fails, and to signal authentication failure to the MPU. One of ordinary skill in the art would have been motivated to employ the teachings of Worley in order to enable operational control

of secure resources without exposing privilege instructions and registers. (see Worley paragraph [0020], lines 16-21)

Regarding Claim 4, Ellison discloses the method of claim 1, further comprising providing isolation by partitioning a local memory into a general communication region and a region accessible only by the APU. (see Ellison col. 4, lines 16-22: partitioned memory, isolated and non-isolated)

Regarding Claim 6, Ellison discloses a system for authenticating code or data within a dynamically allocated partition in a local store, comprising:

a) the local store, wherein the local store is partitioned into an isolated and non-isolated region; (see Ellison col. 4, lines 16-22: dynamically partitioned memory, isolated and non-isolated)

c) an attached processor (APU) coupled to the local store, the APU configured to execute the authenticated code in the local store. (see Ellison col. 5, lines 43-46: processor coupled to memory; col. 6, lines 5-10: execute image)

Ellison discloses wherein a load and exit state machine employable to load the code or data to the isolated region of the local store, the load and exit state machine further employable to verify contents of the local store. (see Ellison col. 3, lines 21-25; col. 3, lines 45-47: load code and data to isolated region, verify load image) Ellison does not specifically disclose authenticate contents of local store.

However, Worley discloses:

b) to authenticate contents of the local store; (see Worley paragraph [0049], lines 1-7; paragraph [0129], lines 9-15; paragraph [0139], lines 27-33: authentication image, failure indication)

It would have been obvious to one of ordinary skill in the art to modify Ellison as taught by Worley to enable the capability to authenticate the contents of local store. One of ordinary skill in the art would have been motivated to employ the teachings of Worley in order to enable operational control of secure resources without exposing privilege instructions and registers. (see Worley paragraph [0020], lines 16-21)

Regarding Claim 7, Ellison discloses the system of claim 6, wherein the APU is isolated. (see Ellison col. 4, line 63 - col. 5, line 5: isolated processor, specific operation mode)

Regarding Claim 8, Ellison discloses the system of claim 1, wherein the APU is further configured to issue a local store de-isolate command. (see Ellison col. 3, lines 43-45; col. 5, lines 5-10: command (i.e. instruction) processing, initiate/exit isolated mode)

Regarding Claim 10, Ellison discloses the system of claim 6, further comprising a main processor unit (MPU) indirectly coupled to the local store. (see Ellison col. 5, lines 43-46: processor coupled to memory)

Regarding Claim 11, Ellison discloses the system of claim 6, wherein the APU is configured to deny the MPU access to indicia within the isolated region of the local store. (see Ellison col. 6, lines 13-18: access restricted to isolated region)

Regarding Claim 12, Ellison discloses a method for dynamically partitioning and un-partitioning a local store for the authentication of code or data, comprising:

a) partitioning the local store into an isolated and non-isolated section; (see Ellison col. 4, lines 16-22: partitioned memory, isolated and non-isolated)
b) loading code or data into the isolated section; (see Ellison col. 3, lines 45-47: load image)

Ellison discloses wherein verifying the code or data into the isolated section of local store. (see Ellison col. 3, lines 45-47: verifies (i.e. authenticate) load image, authentication verified) Ellison does not specifically disclose authenticating the code or data into the isolated section of the local store.

However, Worley discloses:

c) authenticating the code or data into the isolated section of the local store. (see Worley paragraph [0049], lines 1-7; paragraph [0129], lines 9-15; paragraph [0139], lines 27-33: authentication code)

It would have been obvious to one of ordinary skill in the art to modify Ellison as taught by Worley to enable the capability to authenticate the code or data into the isolated section of the local store. One of ordinary skill in the art would have been

motivated to employ the teachings of Worley in order to enable operational control of secure resources without exposing privilege instructions and registers. (see Worley paragraph [0020], lines 16-21)

Regarding Claim 13, Ellison discloses the method of claim 12, wherein the partitioning of the local store is initiated by a load command. (see Ellison col. 5, lines 5-10; col. 3, lines 43-45: partitioning isolated region, initiation or configuration command)

Regarding Claim 14, Ellison discloses the method of claim 13, wherein the load command is issued by a main processor unit (MPU). (see Ellison col. 3, lines 43-45: load command initiated by processor)

Regarding Claim 15, Ellison discloses the method of claim 8, further comprising code or data in the isolated section of the local store. (see Ellison col. 4, lines 16-22: code or data in isolated region; col. 5, lines 5-10: execute loaded image) Ellison does not specifically disclose executing authenticating code or data into the isolated section of the local store. However, Worley discloses wherein executing authenticated code or data, and in the isolated section of the local store. (see Worley paragraph [0049], lines 1-7; paragraph [0129], lines 9-15; paragraph [0139], lines 27-33: authentication code executed)

It would have been obvious to one of ordinary skill in the art to modify Ellison as taught by Worley to enable the capability to execute authentication code or data in an

isolated region. One of ordinary skill in the art would have been motivated to employ the teachings of Worley in order to enable operational control of secure resources without exposing privilege instructions and registers. (see Worley paragraph [0020], lines 16-21)

Regarding Claim 16, Ellison discloses the method of claim 15, further comprising erasing code or data in the isolated section of the local store after executing the authenticated code. (see Ellison col. 5, lines 5-10; col. 3, lines 43-45: configuration commands, initialize or reset isolated region) Ellison does not specifically disclose executing the authentication code. However, Worley disclose wherein executing the authentication code. (see Worley paragraph [0049], lines 1-7; paragraph [0129], lines 9-15; paragraph [0139], lines 27-33: authentication code executed)

It would have been obvious to one of ordinary skill in the art to modify Ellison as taught by Worley to enable the capability to execute the authentication code. One of ordinary skill in the art would have been motivated to employ the teachings of Worley in order to enable operational control of secure resources without exposing privilege instructions and registers. (see Worley paragraph [0020], lines 16-21)

Regarding Claim 17, Ellison discloses the method of claim 16, further comprising de-partitioning the local store into a non-isolated state. (see Ellison col. 4, lines 16-22: partitioned memory, isolated and non-isolated regions)

Regarding Claim 18, Ellison discloses the method of claim 17, wherein the de-partitioning is started through execution of an exit command. (see Ellison col. 5, lines 5-10; col. 3, lines 43-45: command processing, isolated region)

Regarding Claim 19, Ellison discloses the method of claim 12, further comprising:

a) using the master key to decrypt at least one encrypted key from the loaded code; (see Ellison col. 10, lines 6-8; col. 9, lines 64-65; col. 10, lines 16-19: decryption (i.e. key) utilized loading image) and

b) decrypting additional loaded code or data with the at least one decrypted key. (see Ellison col. 10, lines 6-8; col. 9, lines 64-65; col. 10, lines 16-19: decryption (i.e. key) utilized loading image)

Regarding Claim 20, Ellison discloses a processor for dynamically partitioning a local store for the authentication of code or data, the processor including a computer program, comprising:

a) computer code for partitioning an attached processor unit (APU) into an isolated and non-isolated section; (see Ellison col. 7, lines 41-43: software to implement; col. 4, lines 16-22: partitioning memory, isolated and non-isolated regions)

b) computer code for loading code or data into the isolated section; (see Ellison col. 7, lines 41-43: software to implement; col. 3, lines 21-25; col. 3, lines 45-47: load code or data into isolated region) and

Ellison discloses the capability to verify a software module (i.e. load image) (see Ellison col. 3, lines 45-47: verifies (i.e. authenticate) load image; col. 5, lines 5-10: execute loaded image), and computer code. (see Ellison col. 7, lines 41-43: software to implement) Ellison does not specifically disclose authenticating code or data into the isolated section.

However, Worley discloses:

c) authenticating code or data into the isolated section. (see Worley paragraph [0049], lines 1-7; paragraph [0129], lines 9-15; paragraph [0139], lines 27-33: authentication code)

It would have been obvious to one of ordinary skill in the art to modify Ellison as taught by Worley to enable the capability for authenticating code or data into the isolated section. One of ordinary skill in the art would have been motivated to employ the teachings of Worley in order to enable operational control of secure resources without exposing privilege instructions and registers. (see Worley paragraph [0020], lines 16-21)

Regarding Claim 21, Ellison discloses a computer program product for dynamically partitioning a local store for the authentication of code or data in a computer system, the computer program product having a medium with a computer program embodied thereon, the computer program comprising:

a) computer code for partitioning an attached processor unit (APU) into an isolated and non-isolated section; (see Ellison col. 7, lines 41-43: software to implement; col. 3, lines 4-8; col. 4, lines 16-22: partitioning system, memory and execution)

b) computer code for loading code into the isolated section; (see Ellison col. 7, lines 41-43: software to implement; col. 3, lines 21-25; col. 3, lines 45-47: load image into isolated state)

Ellison discloses the capability to verify a software module (i.e. load image) (see Ellison col. 3, lines 45-47: verifies (i.e. authenticate) load image; col. 5, lines 5-10: execute loaded image), and computer code. (see Ellison col. 7, lines 41-43: software to implement) Ellison does not specifically disclose authenticating code in the isolated section.

However, Worley discloses:

c) authenticating code in the isolated section. (see Worley paragraph [0049], lines 1-7; paragraph [0129], lines 9-15; paragraph [0139], lines 27-33: authentication code)

It would have been obvious to one of ordinary skill in the art to modify Ellison as taught by Worley to enable the capability to authenticate code in the isolated section. One of ordinary skill in the art would have been motivated to employ the teachings of Worley in order to enable operational control of secure resources without exposing privilege instructions and registers. (see Worley paragraph [0020], lines 16-21)

5. Claims **5, 9** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Ellison-Worley** and further in view of **Dahan et al.** (US PGPUB No. **20030140244**).

Regarding Claim 5, Ellison discloses the method of claim 4, further comprising providing isolation. (see Ellison col. 3, lines 4-8; col. 4, lines 16-22: providing isolation) Ellison-Worley does not specifically disclose the capability whereby disabling pervasive and or debug interfaces on the APU. However, Dahan discloses wherein disabling pervasive and or debug interfaces on the APU. (see Dahan paragraph [0064], lines 1-6; paragraph [0064], lines 10-11; paragraph [0085], lines 8-12: enable/disable debug interface)

It would have been obvious to one of ordinary skill in the art to modify Ellison-Worley as taught by Dahan to enable the capability for disabling pervasive and or debug interfaces. One of ordinary skill in the art would have been motivated to employ the teachings of Dahan in order to optimize performance of applications with improvements in security mechanisms to support secure environments. (see Dahan paragraph [0002], lines 1-3: " ... *more specifically to improvements in security mechanisms to support secure software services.* ... "; paragraph [0003], lines 9-12: " ... *optimize the performance of the applications concerned and to achieve this they employ more specialized execution units and instruction sets. Particularly in applications such as mobile telecommunications, but not exclusively, it is desirable to provide ever-increasing DSP performance while keeping power consumption as low as possible.* ... ")

Regarding Claim 9, Ellison discloses the system of claim 5, wherein the APU is further configured to issue an erase command for the isolated partition. (see Ellison col. 3, lines 43-45; col. 5, lines 5-10: command processing, reinitiate (i.e. erase and reset))

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton Johnson whose telephone number is 571-270-1032. The examiner can normally be reached Monday through Friday from 8:00AM to 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar Moazzami, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

C.J.

Carlton Johnson
November 21, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

11/27/06